(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01827 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/18676

(22) International Filing Date: 7 June 2001 (07.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/603,878 26 June 2000 (26.06.2000) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LORTZ, Victor** [US/US]; 7716 SW Oviatt Drive, Beaverton, OR 97007 (US). **JASON, James, Jr.** [US/US]; 1613 Glen Ellen Drive, Hillsboro, OR 97142 (US). **SAINT-HILAIRE, Ylian** [CA/US]; 1316 NE Carlaby Way #173, Hillsboro, OR 97124 (US).

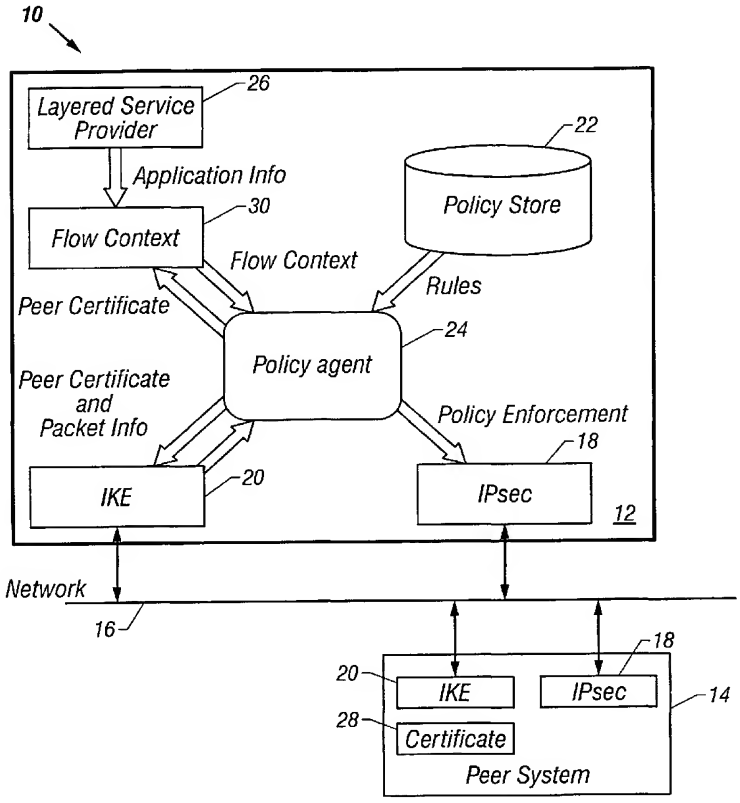
(74) Agent: **HARRIS, Scott, C.**; Fish & Richardson, Suite 500, 4350 La Jolla Village Drive, San Diego, CA 92122 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ESTABLISHING NETWORK SECURITY USING INTERNET PROTOCOL SECURITY POLICIES



(57) Abstract: Techniques for configuring network security include obtaining non-packet flow information, evaluating a policy rule based on the obtained information, and proposing a security arrangement based on the evaluation. The non-packet flow information can include, for example, authentication information obtained during an Internet Key Exchange protocol session or information obtained from a layered service provider. Therefore, policies such as Internet Protocol security (IPsec) policies can be defined and implemented so that they more accurately reflect the network's security requirements.

WO 02/01827 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ESTABLISHING NETWORK SECURITY USING INTERNET PROTOCOL SECURITY POLICIES

BACKGROUND

The invention relates to establishing network security using Internet Protocol security (IPsec) policies.

IPsec is a network-layer security framework for implementing security for communications on networks using the Internet Protocol (IP) through the use of cryptographic key management procedures and protocols. Communications between two endpoints of an IP traffic flow are made secure by the IPsec protocol on an individual IP packet basis. IPsec entities at connection endpoints have access to and participate in operations that make a common connection secure.

IPsec establishes and uses a security association to identify a secure channel between two endpoints. A security association is a unidirectional session between two termination endpoints. One endpoint sends IP packets, and a second endpoint receives the IP packets. A minimum of two security associations is required for secure, bi-directional communications. The two endpoints can use the Internet Key Exchange (IKE) protocol to negotiate mutually acceptable

encryption algorithms, associated parameters and secret keys to protect network traffic. The IKE protocol supports various authentication mechanisms including pre-shared keys, X.509 public key certificates and Kerberos tickets.

Policy-based network management (PMNM) often is used to determine who can use the resources and services associated with the network, under what conditions they are used, and when. Security policies, for example, define a set of rules governing encryption and access control decisions. The policies can be expressed as a set of rules each of which includes a predicate and an action. In other words, a rule can be expressed as "if <condition> is satisfied, then do <action>."

An exemplary action at the IPsec layer may propose a specific set of security algorithms. Current IPsec protocol implementations typically use packet flow information, such as IP addresses, protocol and ports, to evaluate the policy decisions.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a system including IPsec-enabled devices.

FIG. 2 is a flow chart of a method of establishing a security association.

FIG. 3 illustrates workgroups in a policy-based network management infrastructure.

FIG. 4 shows a set of rules associated with the workgroups in FIG. 3.

DETAILED DESCRIPTION

FIG. 1 illustrates a system 10 with IPsec-enabled devices 12, 14 that can communicate over a network 16. Each of the devices 12, 14 includes a layered protocol stack that has an IPsec component 18 and an IKE component 20. The device 12 also includes a database 22 that stores rules corresponding to security policies for implementing the security requirements of the device. A policy agent 24 retrieves the rules stored by the database 22 and interprets and evaluates the rules. As described in greater detail below, the policy agent 24 can exchange information with the IKE layer component 20, as well as various information providers, to augment the network flow information that drives the policy decisions.

As indicated by FIG. 2, when the device 12 attempts to send or receive IP data to the other device 14, the IPsec layer 18 in the device 12 attempts to find 40 a security association, in other words, a set of encryption, authentication and/or compression algorithms and keys, to protect the traffic. If a security association is not yet established, the IPsec layer 18 initiates 42 a process to establish one or more security associations to be used for future traffic that matches the same IP address, port and protocol. The IKE protocol is used to negotiate the keys and algorithms of the security associations. During a first IKE phase, the devices 12, 14 exchange and authenticate identity information and establish a secure channel protected by an IKE security association to use for a second IKE phase. During the second phase, the devices 12, 14 negotiate security associations for the IP traffic that is to be protected by IPsec.

As noted, during the first IKE phase, the IKE layer 20 in the device 12 obtains 44 authenticated identity information 28 from the device 14. The identity information can include, for example, a digital certificate, a username-password pair or a Kerberos ticket. The identity information can identify a peer device and may be associated with a particular device such as

the device 14 or a group of devices. Alternatively, the identity information may be associated with a particular individual or group of individuals. For example, a hospital may have doctors, nurses and administrative staff organized in workgroups each of which may have specific access privileges and security requirements. The identity information can be associated with a particular group of the hospital staff. FIG. 3 illustrates three exemplary workgroups in a policy-based network management infrastructure. Each client (machine or user) in a workgroup has an ordered list of policy objects, and each policy object includes a set of rules to apply to traffic flows between two endpoint lists. For example, the source list can identify machines in the source workgroup, whereas the destination list can identify machines in the destination workgroup. Smart cards, which can store certificates in a secure manner, can enable tying the certificate to one or more users rather than to the machines. The certificate would then identify the user or the machine as being a member of a particular workgroup. The non-packet flow information can include biometric data that identifies the user as well.

Once the IKE layer 20 in the device 12 obtains the authenticated identity information, the identity information

is obtained 46 by the policy agent 24. The IKE layer 20 can include an application programming interface (API) to allow the policy agent 24 to extract the authenticated identity information. Alternatively, the IKE layer 20 can send the authenticated identity information to the policy agent. The policy agent 24 can use the identity information to interpret and evaluate 48 policies that are stored in the database 22 and that include a condition referring to the IKE layer identity information. For example, a particular policy may indicate that if the identity information includes a particular digital certificate, then traffic must be sent in the clear, denied or secured using a set of security parameters. Exemplary forms for the rules associated with one of the workgroups of FIG. 3 are shown in FIG. 4. In general, the sets of rules should be symmetrical and synchronized across all the workgroups.

The policy agent 24 also can pass 50 the authenticated identity information to a flow context module 30 which may reside within the policy agent or which may be separate from the policy agent. The module 30, which can be implemented, for example, in random access memory (RAM), serves as a repository for information that can flow to the policy agent 24. The module 30 also can obtain additional information from

other sources, such as a layered service provider 26 or other network interceptor. The information obtained from the layered service provider 26 then can be passed 52 to the policy agent 24 and used to evaluate 54 IPsec policies stored in the database 22. That allows IPsec policies to be based on a specific application, as well as the identity of the logged-in user and/or peer identities. For example, in some implementations, the layered service provider 26 would determine that a certain application is responsible for a specific connection request and would advertise the application's name as "Application = XYZ." The form in which the extended information is represented can be similar to the form in which the identity information is represented. Therefore, the same syntax can be used when incorporating the IKE layer identity information or the information from the layered service provider 26 into predicates in the policies. Some sources of context information, such as user-loadable programs and dynamic link libraries (DLLs) may require authentication by the policy evaluator to certify the reliability of the information they provide. Such authentication can be provided using bilateral software authentication technology. Preferably, information obtained from other sources such as the layered service provider 26 is

used to augment, but not override, values in the authenticated identity information obtained from the IKE layer 20.

The non-packet flow information that is received, for example, through the flow context module 30 can be viewed as a set of attributes each of which has an associated value. The packet flow itself is identified by several parameters, including a source address, a source port, a destination address, a destination port and a protocol. Those parameters can be added to the flow context information so that as data packets are processed, there is sufficient information to look up the corresponding flow context information to evaluate the policy rules. Such a technique can facilitate integration of the non-packet flow information with the packet flow information.

Once the policy agent 24 evaluates the policies in the database 22, the policy agent 24 passes 56 a prioritized list of one or more protection suite proposals to the IKE layer 20 in the device 12. The IKE layer 20 in the device 12 then passes 58 the prioritized list of protection suite proposals to the IKE layer 20 in the device 14. The device 14 examines 60 the proposed protection suites and attempts to find an acceptable protection suite on the list. Once the devices 12, 14 agree on an acceptable security arrangement, the IPsec

layer 18 in each device is configured 62 to use the agreed-upon suite of security arrangements during the second phase of the IKE protocol.

As mentioned previously, various types of non-packet flow information can be incorporated into the predicates of IPsec policies. Specific examples include user identity data, application identifiers, and application modes. User identity data, for example, can be obtained from smart cards or biometric devices. Such identity data also can include a password entered, for example, when the user logs on to the system. The digital certificate information can include fields such as the certificate serial number, the subject's name, the subject's public key, the subject's alternate names, key identifiers and the expiration date of the certificate. The information in any of those fields can be incorporated into the predicates of one or more policy rules, and the received digital certificate can be used to evaluate the rules.

If the IKE layer 20 in the first device is unable to authenticate identity information from the second device 14 during the IKE session, then the IKE layer itself may act as an information provider. For example, the IKE layer 20 can indicate to the policy agent 24 that authenticated identity

information is unavailable for the particular connection request. The policy agent 24 would then use that fact to evaluate one or more default policies in the database 22.

In one particular scenario, an application identifier can be used to evaluate IPsec policies as follows. An application (not shown) loads a layered service provider DLL automatically as it loads Winsock 2 to perform network communications. The layered service provider hashes the application binary executable file and looks it up in a database of known applications. The layered service provider then signs the application identifier and passes the signed value to the module 30 along with the packet flow information (i.e., address, port and protocol). The module 30 creates a record for the data flow, checks the validity of the application identifier, and adds the identifier to the flow context. As the policy agent 24 evaluates the policies in the database 22, rules that specify an application identifier are evaluated against the application identifier in the context record.

An application also can declare and sign the mode in which it is running. Examples include a browser running in Secure Socket Layer (SSL), an electronic mail (e-mail) application sending or receiving messages, and a browser accessing web sites on a particular domain. As the policy

agent 24 evaluates the policies in the database 22, rules that specify an application mode are evaluated against the actual mode in which the application is running.

Although the foregoing description relates to the use of non-packet flow information to evaluate policies and negotiate a security association during the first phase of an IKE session, the non-packet flow information also can be used during subsequent phases of an IKE session to evaluate policies and negotiate security associations.

Various features of the system can be implemented in hardware, software, or a combination of hardware and software. For example, some aspects of the system can be implemented in computer programs executing on programmable computers. Each program can be implemented in a high level procedural or object-oriented programming language to communicate with a computer system. Furthermore, each such computer program can be stored on a storage medium, such as read-only-memory (ROM) readable by a general or special purpose programmable computer, for configuring and operating the computer when the storage medium is read by the computer to perform the functions described above.

Other implementations are within the scope of the following claims.

What is claimed is:

1. A method of establishing network security comprising:

obtaining non-packet flow information;

evaluating a policy rule based on the obtained information; and

proposing a security arrangement based on the evaluation.

2. The method of claim 1 wherein the non-packet flow information includes peer identity information.

3. The method of claim 1 wherein the non-packet flow information includes user identity information.

4. The method of claim 3 including obtaining the user identity information from a smart card.

5. The method of claim 3 wherein the non-packet flow information includes biometric data.

6. The method of claim 1 wherein the non-packet information includes authenticated identity information obtained during an Internet Key Exchange protocol session.

7. The method of claim 6 wherein the identity information is included in a digital certificate.

8. The method of claim 6 wherein the identity information is included in a Kerberos ticket.

9. The method of claim 1 including obtaining the non-packet flow information from a network interceptor.

10. The method of claim 1 wherein the non-packet flow information includes an application identifier.

11. The method of claim 1 wherein the non-packet flow information includes an identification of a mode in which an application is executing.

12. The method of claim 1 including configuring an Internet Protocol security layer according to the proposed security arrangement.

13. A security-enabled device comprising:

a protocol stack;

a database of policy rules; and

a policy agent configured to obtain non-packet flow information received from a second device, evaluate a policy rule stored in the database based on the obtained information, and propose a security arrangement based on the evaluation for future communications with the second device.

14. The device of claim 13 wherein the policy agent is configured to receive non-packet flow information from a network interceptor and to evaluate a policy rule stored in the database based on the received information, wherein the proposed security arrangement depends on the received non-packet flow information.

15. The device of claim 13 wherein the policy agent is arranged to configure an Internet Protocol security component according to the proposed security arrangement if, during an Internet Key Exchange session, the second device agrees to use the proposed security arrangement.

16. An article comprising a computer-readable medium that stores computer-executable instructions for causing a computer system to:

obtain non-packet flow information;

evaluate a policy rule based on the obtained information; and

propose a security arrangement based on the evaluation.

17. The article of claim 16 wherein the non-packet flow information includes peer identity information.

18. The article of claim 16 wherein the non-packet flow information includes user identity information.

19. The article of claim 16 wherein the non-packet information includes authenticated identity information obtained during an Internet Key Exchange protocol session.

20. The article of claim 19 wherein the identity information is included in a digital certificate.

21. The article of claim 19 wherein the identity information is included in a Kerberos ticket.

22. The article of claim 16 wherein the non-packet flow information is obtained from a layered service provider.

23. The article of claim 16 wherein the non-packet flow information includes an application identifier.

24. The article of claim 16 wherein the non-packet flow information includes biometric data.

25. The article of claim 16 wherein the non-packet flow information includes an identification of a mode in which an application is executing.

26. The article of claim 16 including instructions to configure an Internet Protocol security layer according to the proposed security arrangement if, during an Internet Key Exchange session, a second device agrees to use the proposed security arrangement.

27. A communications system comprising:

first and second Internet Protocol security-enabled devices, wherein both devices include respective protocol stacks having an Internet Key Exchange component and an Internet Protocol security component; and

a network over which the first and second devices can communicate,

wherein the first device further includes a database of policy rules and a policy agent, wherein the policy agent is configured to obtain non-packet flow information received by the first device's Internet Key Exchange component from the second device's Internet Key Exchange component, to evaluate a policy rule stored in the database based on the obtained information, and to propose an Internet Protocol security arrangement based on the evaluation for future communica-tions in an Internet Key Exchange session with the second device.

28. The system of claim 27 wherein the policy agent is configured to receive non-packet flow information from a network interceptor and to evaluate a policy rule stored in the database based on the received information, wherein the proposed security arrangement depends on the received non-packet flow information.

29. The system of claim 27 wherein the policy agent is arranged to configure the first device's Internet Protocol security component according to the proposed security arrangement if, during an Internet Key Exchange session, the second device agrees to use the proposed security arrangement.

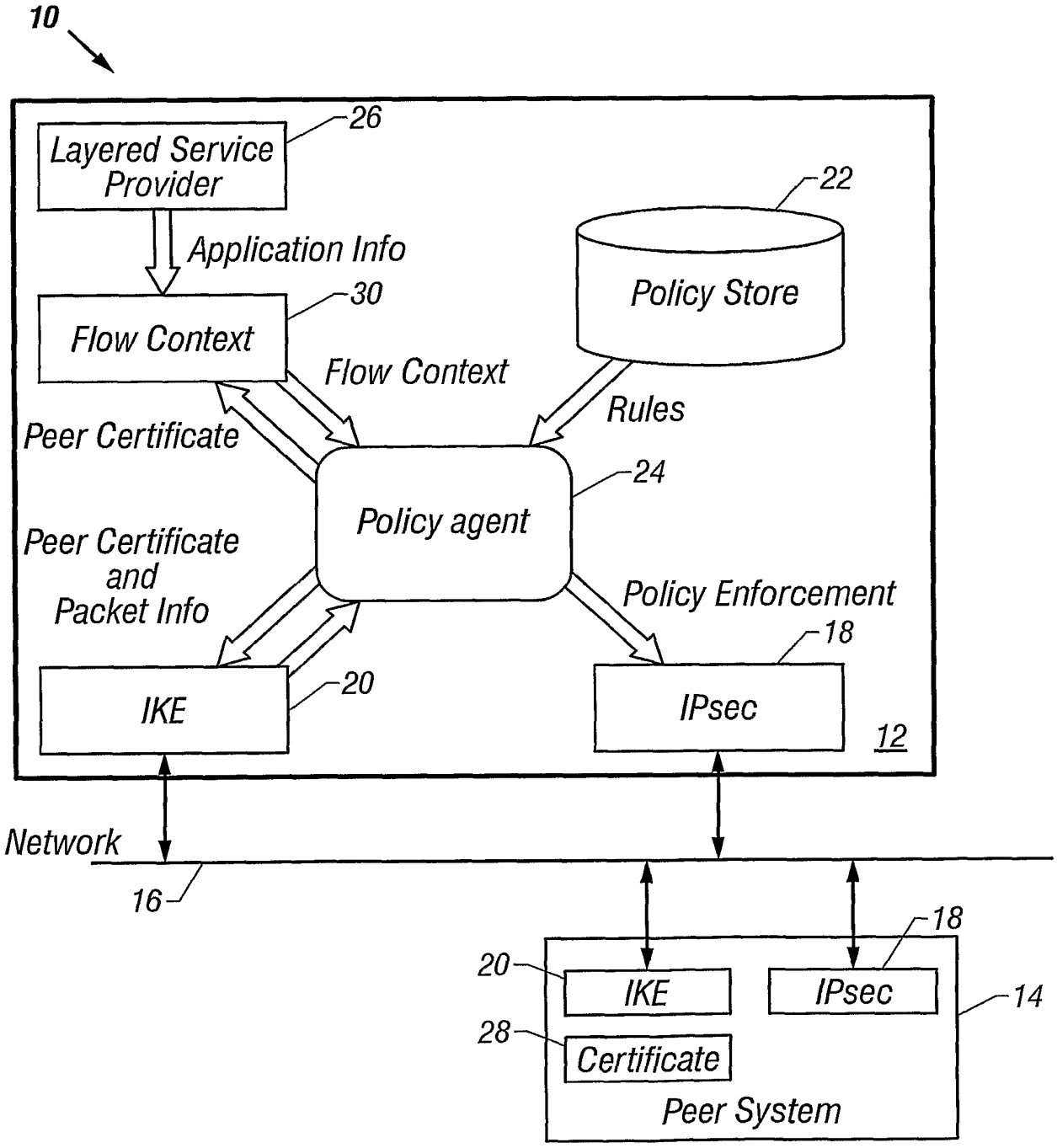

10
Layered Service Provider
26
Application Info
Flow Context
30
Flow Context
Peer Certificate
Policy Store
22
Rules
Policy agent
24
Peer Certificate and Packet Info
Policy Enforcement
IKE
20
IPsec
18
12
Network
16
20
IKE
IPsec
18
14
28
Certificate
Peer System

FIG. 1

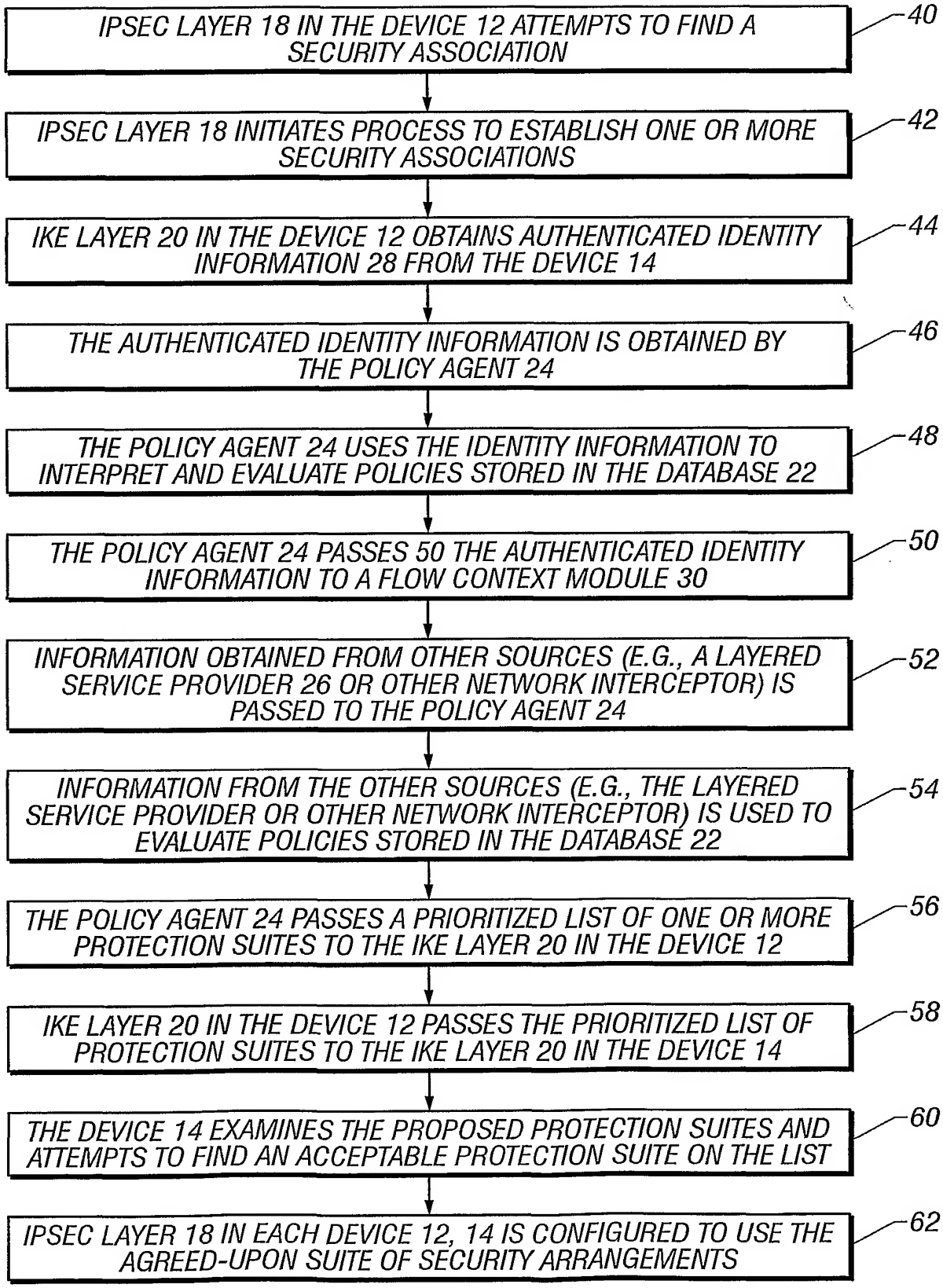

IPSEC LAYER 18 IN THE DEVICE 12 ATTEMPTS TO FIND A SECURITY ASSOCIATION
40
IPSEC LAYER 18 INITIATES PROCESS TO ESTABLISH ONE OR MORE SECURITY ASSOCIATIONS
42
IKE LAYER 20 IN THE DEVICE 12 OBTAINS AUTHENTICATED IDENTITY INFORMATION 28 FROM THE DEVICE 14
44
THE AUTHENTICATED IDENTITY INFORMATION IS OBTAINED BY THE POLICY AGENT 24
46
THE POLICY AGENT 24 USES THE IDENTITY INFORMATION TO INTERPRET AND EVALUATE POLICIES STORED IN THE DATABASE 22
48
THE POLICY AGENT 24 PASSES 50 THE AUTHENTICATED IDENTITY INFORMATION TO A FLOW CONTEXT MODULE 30
50
INFORMATION OBTAINED FROM OTHER SOURCES (E.G., A LAYERED SERVICE PROVIDER 26 OR OTHER NETWORK INTERCEPTOR) IS PASSED TO THE POLICY AGENT 24
52
INFORMATION FROM THE OTHER SOURCES (E.G., THE LAYERED SERVICE PROVIDER OR OTHER NETWORK INTERCEPTOR) IS USED TO EVALUATE POLICIES STORED IN THE DATABASE 22
54
THE POLICY AGENT 24 PASSES A PRIORITIZED LIST OF ONE OR MORE PROTECTION SUITES TO THE IKE LAYER 20 IN THE DEVICE 12
56
IKE LAYER 20 IN THE DEVICE 12 PASSES THE PRIORITIZED LIST OF PROTECTION SUITES TO THE IKE LAYER 20 IN THE DEVICE 14
58
THE DEVICE 14 EXAMINES THE PROPOSED PROTECTION SUITES AND ATTEMPTS TO FIND AN ACCEPTABLE PROTECTION SUITE ON THE LIST
60
IPSEC LAYER 18 IN EACH DEVICE 12, 14 IS CONFIGURED TO USE THE AGREED-UPON SUITE OF SECURITY ARRANGEMENTS
62

FIG. 2

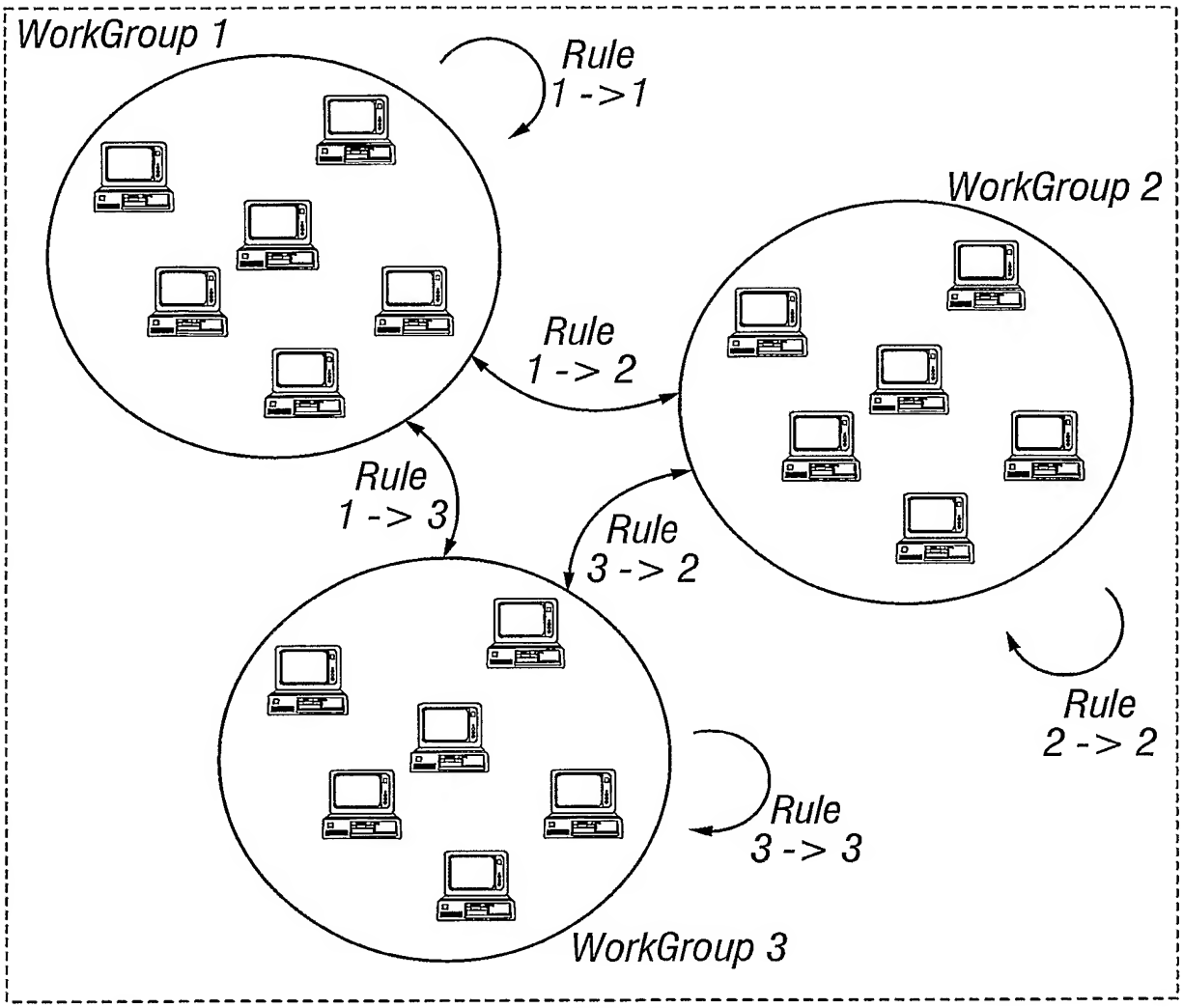


FIG. 3

Policy Object 1 From Workgroup 1 (Endpoint List S_{11} ... S_{1n}) to Workgroup 1 (Endpoint List S_{11} ... S_{1n}) Apply ruleset X11
Policy Object 2 From Workgroup 1 (Endpoint List S_{11} ... S_{1n}) to Workgroup 2 (Endpoint List S_{21} ... S_{2n}) Apply ruleset X12
Policy Object 3 From Workgroup 1 (Endpoint List S_{11} ... S_{1n}) to Workgroup 3 (Endpoint List S_{31} ... S_{3n}) Apply ruleset X13

FIG. 4